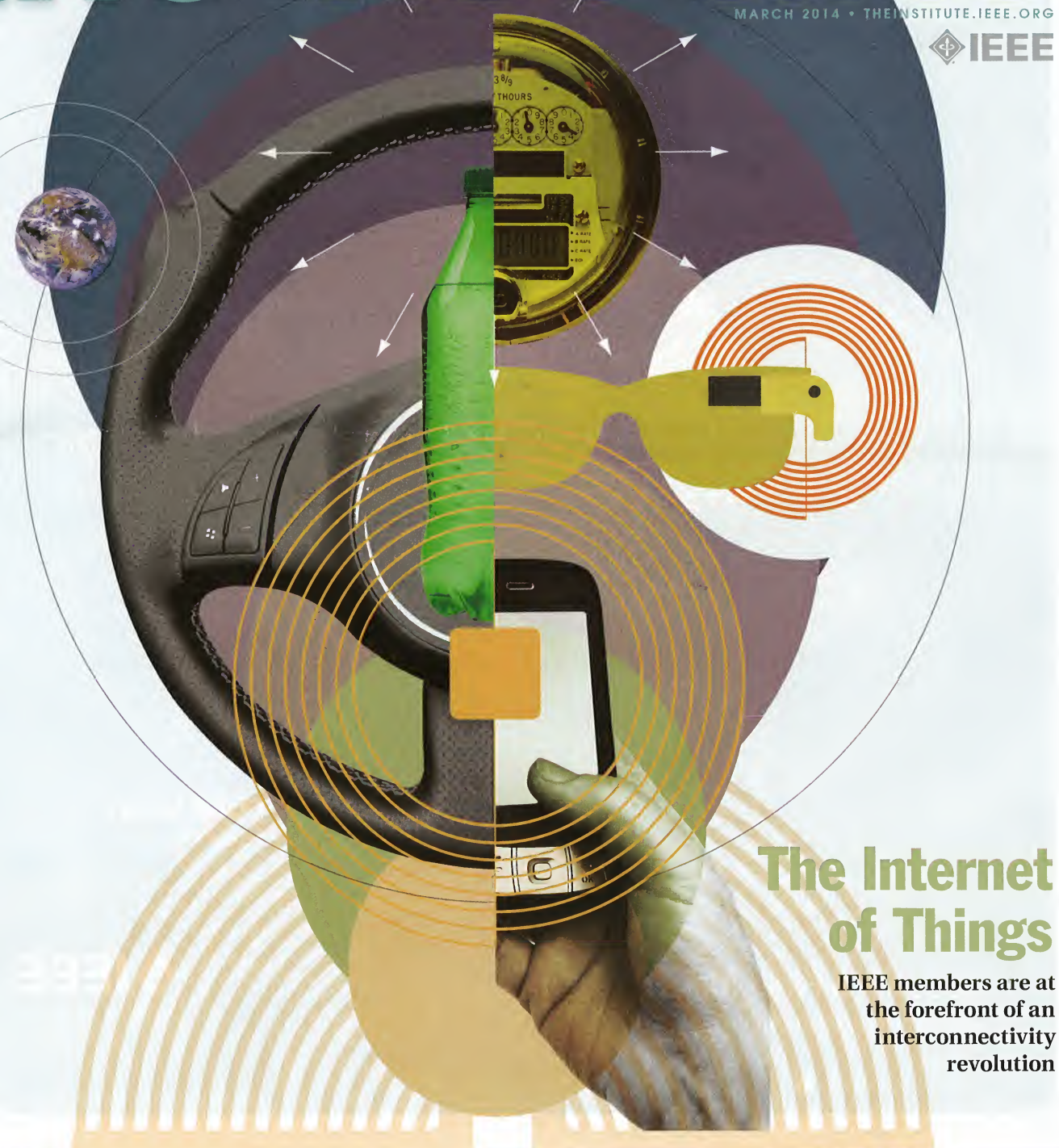
the institute

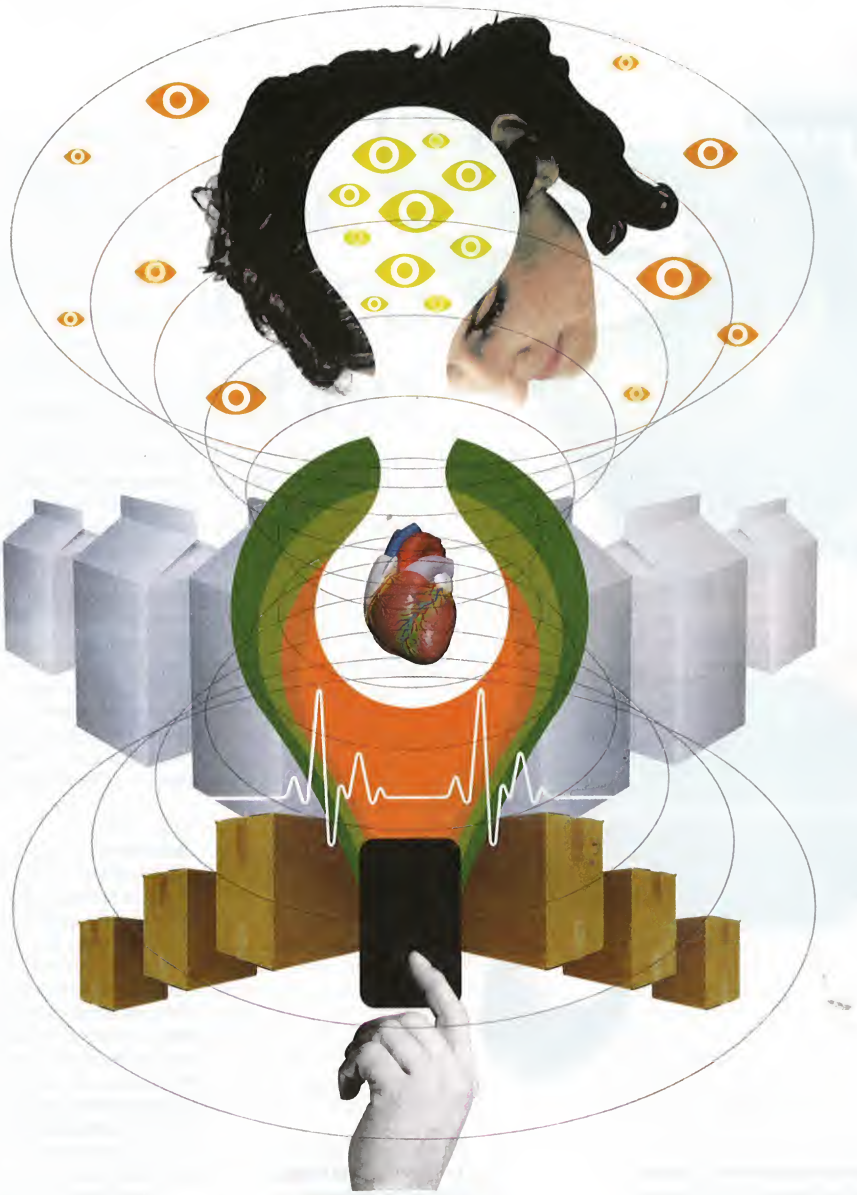
MARCH 2014 • THEINSTITUTE.IEEE.ORG

IEEE



The Internet of Things

IEEE members are at the forefront of an interconnectivity revolution



TECH TOPIC

The Value of Privacy

Safeguarding your information in the age of the Internet of Everything

BY MONICA ROZENFELD

THE INTERNET OF Things promises many advances, such as the ability for consumers to keep track of their energy usage on their phones or receive alerts when milk is running low. Everything, including our homes and our heartbeats, will be monitored to make our lives easier and healthier.

But with the IoT, or what some call the "Internet of Everything," companies are planning to turn information about our every move into valuable market data. Soon, personalized ads—like those that follow online users from one website to the next—are likely to follow us in text messages and on face-scanning screens as we walk down store aisles. Information such as the purchases we make, our genders and ages, and the places we frequent will be collected to inform us—whether we care to know or not—what we might want to buy next. Although some argue that this brings added value by personalizing the shopping experience, others believe such uses of the IoT are invasions of privacy.

"Privacy as we know it will have to be completely redefined," says IEEE Senior Member Raul Colcher, CEO of Questera, an information technology consulting company in Rio de Janeiro. He advises businesses on how to handle privacy and security as the IoT evolves.

"The Internet of Things will create a completely new scenario for

STUART BRADFORD

and security that will need dressed," Colcher says. He t we are already dealing ted issues, including com- ollecting information about our online activity. But with more of our information vailable. We're likely to be inders that, for example, nning low on shampoo or due for a vacation.

TURE IS HERE

T applications are already nsor technology products ter homes, for example, vide families with peace of s their ads suggest. With ick on a mobile device, n activate a security sys- home, turn off lights while vacation, turn up the ther- on a cold night while still an m home, or lock the front m the driveway. Signals those sensors travel through s network to be stored in the ith the information analyzed d upon. And that can some- problematic.

is controlling what's in d? Do I trust my cloud- ing system?" asks IEEE Member Neeli Prasad, vice nt at SAI Technology, a er of mobile cloud network in Santa Clara, Calif. "Do I e people who have access to rmation?"

vacy is of great concern, uals may have to become n service providers, says She sees a trend toward loud-computing systems in ndividuals store their infor- privately instead of relying panies. "That way, we can what information leaves es and becomes part of the loud and what doesn't."

y new products on the mar- uding the video-streaming Hulu and the Nike Fuelband, nonitors exercise activity, give ers the option to sync those s with their social networks and mobile phones, essentially storing that information in cloud systems and databases. Thus, they can share information with the public about what TV shows they watch or how much they exercise. Or not. "Users can deny this option," Prasad says. One example is the recent news that consumers will be able to opt out of Wi-Fi tracking that allows companies to collect information about the places people visit and the purchases they make through their smartphones.

Concern over unauthorized access to private information is not increasing, she says. There is just more of it to worry about. "Sometimes the shadow of a new technology and its applications are scarier than the thing itself," she says. Moreover, not every application is intended to sell us something or observe our private lives. For example, law enforcement can track a missing person by accessing the GPS coordinates in a smartphone. (So can relatives and friends who have security access via a mobile app, such as Find My iPhone.)

A PRECAUTIONARY TALE

Not all are as optimistic as Prasad about the future of the IoT. While users may have control over who in the general public sees their information, the bigger concern for consumer privacy expert Katherine Albrecht is the question of who owns the data. She is an executive with StartPage, a search engine that does not collect or share personal information, and StartMail, an encrypted e-mail service.

An article coauthored with IEEE Senior Member Katina Michael, "Connected: To Everyone and Everything," in the Winter 2013 issue of *IEEE Technology and Society Magazine*, puts Albrecht's concern bluntly: "[Consumers] may think we're in charge of our shopper cards and our mobile apps and our smart fridges—but … let's not fool ourselves. [The information] is not ours. It belongs to Google, and IBM, and Cisco Systems…and the global Mega-Corp that owns your local supermarket. If you don't believe us, just try removing 'your' data from their databases."

Michael is the associate dean international of the University of Wollongong Faculty of Engineering and Information Sciences, in Australia, and editor in chief of *IEEE Technology and Society Magazine*.

To prepare for the interconnected future, businesses and governments are outlining measures to be taken while new policies are developed. The European Union, for example, outlined such measures in its report "IoT Privacy, Data Protection, Information Security," published in January 2013. One recommendation is to develop privacy-friendly default settings on IoT products and services that would give users more control over what information is shared with others. Furthermore, it suggests that IoT networks give individuals the rights to their own data. In 2012, participants at the Open IoT Assembly—an initiative to envision a future with the IoT—developed an "IoT Bill of Rights" at a two-day conference in London that calls for transparency of IoT processes and the preservation of privacy. It also calls for people to have access to their personal data.

Despite potential risks to privacy, companies are betting their customers will see the advantages that the IoT will bring them, says Colcher. But some groups advocate that consumers have the power to slow down or even stop the advancement of the IoT. Not Colcher. "The inclusion of the IoT all around us is inevitable," he says. "The only thing to do now is to prepare the best we can."